CLAIMS

1. A system for integrating a seller':s Web site with a public key infrastructure, the Web site comprising a Web server and a Web application, the public key infrastructure comprising a buyer computer comprising a Web browser adapted to invoke a signing interface to digitally sign electronic messages, the public key infrastructure further comprising a seller's bank computer system adapted to receive service requests from the seller and respond to those requests with digitally signed service responses; the system comprising:

a filter adapted to redirect HTTP requests received from the Web browser;

an Internet server application adapted to receive a redirected HTTP request from the filter and process the redirected HTTP request;

a filter engine adapted to receive the processed HTTP request and identify an HTTP request that contains data requiring signature by the buyer.

2. The system of claim 1, wherein the filter engine is further adapted to identify an HTTP request that requires accessing a service offered by the seller's bank and to formulate a request for the service, and wherein the system further comprises:

a bank interface adapted to receive the request from the filter engine, reformat the request, and transmit the request to the seller's bank.

3. The system of claim 2, wherein the bank interface is further adapted to receive a service response to the request from the seller's bank and forward the response to the filter engine.

4. The system of claim 2, wherein the service is certificate validation.

5. The system of claim 1, further comprising a second Web server adapted to parse requests redirected by the filter.

6. The system of claim 1, wherein services provided by the seller's bank are provided within the context of a four-corner model.

7. The system of claim 6, wherein the four-corner model comprises the buyer, the seller, the seller's bank, and a buyer's bank.

8. The system of claim 1, wherein the filter is implemented using ISAPI.

9. The system of claim 1, wherein the Internet service application is adapted to generate HTTP responses based on data received from the filter engine.

10. The system of claim 1, wherein the Internet server application is adapted to pass a hash table to the filter engine.

11. The system of claim 10, wherein the hash table comprises the headers from the redirected HTTP request.

12. The system of claim 10, wherein the hash table comprises the method of the redirected HTTP request.

13. The system of claim 10, wherein the hash table comprises the content-type of the redirected HTTP request.

14. The system of claim 10, wherein the hash table comprises the buyer computer's IP address.

15. The system of claim 10, wherein the hash table comprises the actual data in the redirected HTTP request.

16. The system of claim 10, wherein the hash table comprises a unique session ID.

17. The system of claim 1, wherein the Internet service application is a servlet.

18. The system of claim 20, wherein the servlet is constructed as a public class object that extends javax.servlet.http.HttpServlet.

19. The system of claim 21, wherein the public class object comprises a callFilterEngine method, a doGet method, a doPost method, a getRequestHeaders method, a

handleRequest method, and init method, a printErrorResponse method, a printPluginPage method, a readMessage method, a readRequestData method, and a setServletHeaders method.

20. The system of claim 1, wherein the filter engine is adapted to return an object to the servlet.

21. The system of claim 20, wherein the object comprises an integer value indicating one of four conditions: that a signature is required on data in the HTTP request, that a response has been received from the seller's bank concerning a service request, that the HTTP request has been passed through to the Web application, or that an error occurred.

22. The system of claim 1, wherein if the integer value indicates that a signature is required on data in the HTTP request then the Internet server application stores a state of the filter engine in a cookie and causes a Web page containing the cookie and an instruction to sign the data to be transmitted to the Web browser.

23. The system of claim 1, wherein the filter engine determines whether an HTTP request contains data requiring signature by applying filtering rules.

24. The system of claim 1, wherein the filter engine is programmed to recognize each HTTP request that includes data requiring signature.

25. The system of claim 1, wherein the filter engine is programmed to recognize HTTP requests transmitted by the Web browser that have been modified to include a special tag that indicates whether the request includes data that requires signature.

26. The system of claim 1, wherein the filter engine is implemented as a public class object that extends java.lang.object.

27. The system of claim 26, wherein the public class object comprises the following methods: a callWebApp method, a getSessionID method, a newRequestHandler method, an oldRequestHandler method, a service method, and a signedRequestHandler method.

28. The system of claim 1, wherein the filter engine provides an abstracted front end interface via java remote method invocation.

29. The system of claim 1, wherein the filter engine employs a rules class.

30. The system of claim 1, wherein the rules class comprises the following methods: a getMode method, a getService method, a readRules method, a rulesMatch method, and a validateRules method.

31. The system of claim 1, wherein the bank interface is designed with a plug-in based architecture.

32. The system of claim 1, wherein the bank interface supports an abstract front-end interface to allow communication via a plurality of middleware technologies.

33. The system of claim 1, wherein the bank interface is adapted to create and transmit OCSP requests.

34. The system of claim 1, wherein the bank interface comprises a certificate status check module.

35. The system of claim 1, wherein the bank interface comprises a public class object that extends java.lang.object.

36. The system of claim 1, wherein the public class object comprises a createOCSPRequest method, a getCertificateID method, a getCertStatus method, a getCertsVerifyMessage method, a getURL method , an isResponseSuccessful method, a logAndBuildReturnObject method, a processOCSP method, a sendAndReceiveMessage method, a serviceRequest method, and a verifyResponseSignature method.

37. A system for integrating a seller's Web site with a public key infrastructure, comprising:

a Web server;

a Web application connected to the Web server, the Web application adapted to identify HTTP requests that include data requiring signature and to create a Web page for transmission to a browser that will cause the browser to invoke a signing interface to sign the data;

the Web application further adapted to identify HTTP requests that require a service provided by an entity other than the seller; and

a bank interface adapted to receive a request for service from the Web application, format and transmit the request, receive a response to the request, and forward the response to the Web application.